DEMO – Device configurations

Contents

[Introduction 1](#_Toc529213281)

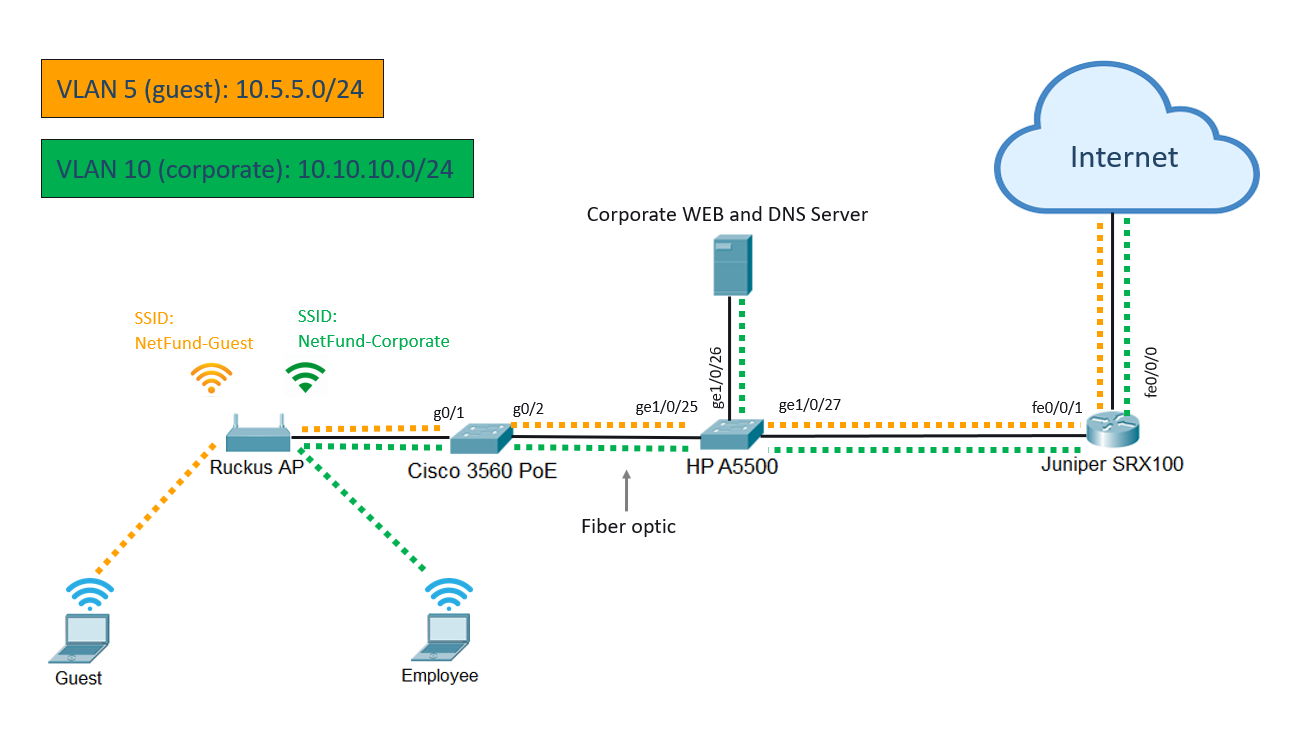
[Juniper SRX100 2](#_Toc529213282)

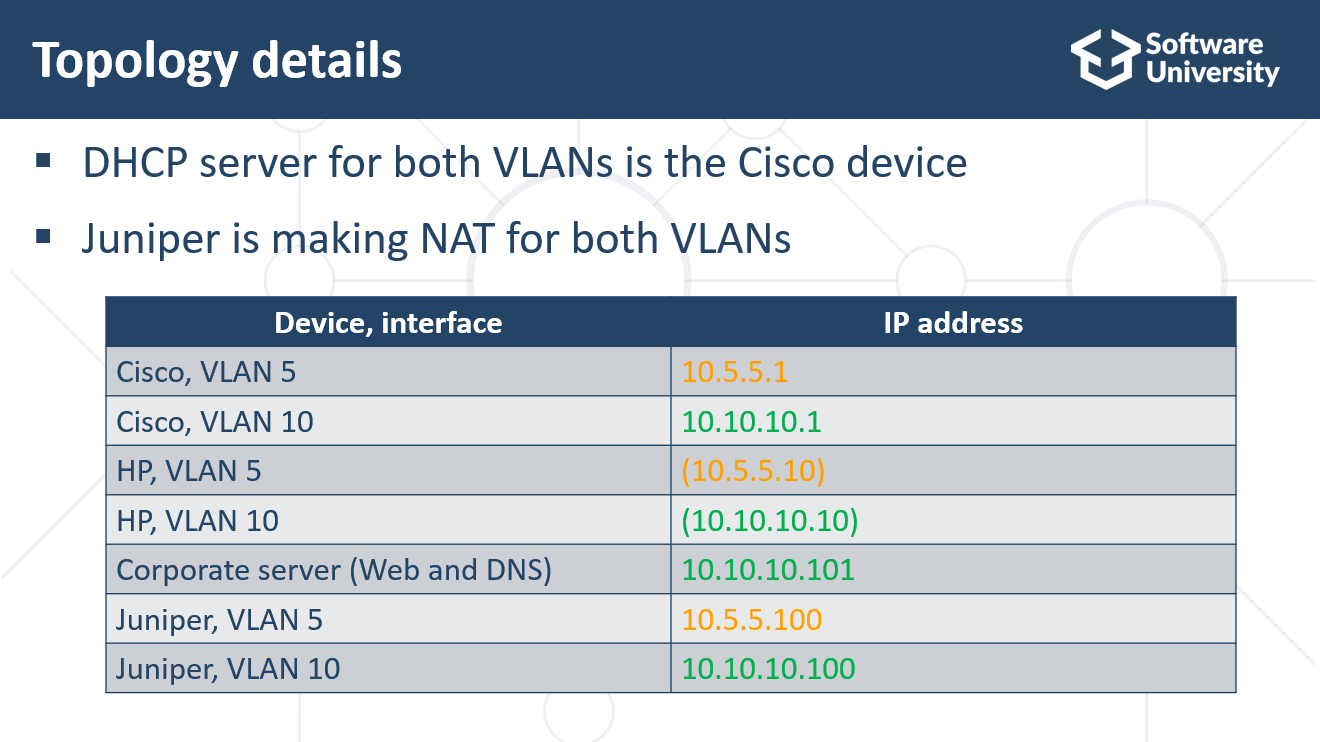
[Cisco 3560-CG PoE 4](#_Toc529213283)

# Introduction

This document does not provide full configurations to be imported in the devices. It provides most of the commands needed for the Juniper and the Cisco devices in order to meet the requirements of the demonstration.

The topology is explained during the course module and you can use the pictures below just for reference. For the details, please have a look at the video for Module 7.





# Juniper SRX100

1. Create vlan 5 and vlan 10

set vlans Vlan5 vlan-id 5

set vlans Vlan vlan-id 10

1. Interfaces:

edit interfaces fe-0/0/1

set vlan-tagging

delete unit 0 family ethernet-switching

set interfaces fe-0/0/1 unit 0 vlan-id 1

set unit 5 vlan-id 5 family inet address 10.5.5.100/24

set unit 10 vlan-id 10 family inet address 10.10.10.100/24

1. Security zones:

set security zones security-zone guest interfaces fe-0/0/1.5

set security zones security-zone corp interfaces fe-0/0/1.10

1. Allow ping

edit security zones security-zone guest

set host-inbound-traffic system-services ping

edit security zones security-zone corp

set host-inbound-traffic system-services ping

1. NAT rules and security policies:

edit security nat source

set rule-set rs1 from zone guest

set rule-set rs1 to zone untrust

set rule-set rs1 rule r1 match source-address 0.0.0.0/0

set rule-set rs1 rule r1 match destination-address 0.0.0.0/0

set rule-set rs1 rule r1 then source-nat interface

set rule-set rs2 from zone corp

set rule-set rs2 to zone untrust

set rule-set rs2 rule r2 match source-address 0.0.0.0/0

set rule-set rs2 rule r2 match destination-address 0.0.0.0/0

set rule-set rs2 rule r2 then source-nat interface

edit security policies from-zone guest to-zone untrust

set policy internet-access match source-address any destination-address any application any

set policy internet-access then permit

edit security policies from-zone corp to-zone untrust

set policy internet-access2 match source-address any destination-address any application any

set policy internet-access2 then permit

Other:

Erase config: load factory-default

set system root-authentication plain-text-password

--

set interfaces fe-0/0/0 unit 0 family inet dhcp

# Cisco 3560-CG PoE

1. Create the VLANs – 5 and 10
2. Make interfaces g0/1 and g0/2 trunks
3. Set IP addresses for VLAN5 (10.5.5.1/24) and VLAN10 (10.10.10.1/24)
4. Create the DHCP Pools:

ip dhcp pool guest

network 10.5.5.0 255.255.255.0

default-router 10.5.5.100

dns-server 8.8.8.8

---

ip dhcp pool corporate

network 10.10.10.0 255.255.255.0

default-router 10.10.10.100

dns-server 10.10.10.101

---

ip dhcp excluded-address 10.5.5.10

ip dhcp excluded-address 10.5.5.100

ip dhcp excluded-address 10.10.10.10

ip dhcp excluded-address 10.10.10.101

ip dhcp excluded-address 10.10.10.100